INFORMATION SECURITY POLICIES

Document Control

Reference Number	SPL/ISMS/POL/ISP/V01
Controls/ Requirement	5.1
Document Owner	ISMS Manager
Classification	Internal Use
Version	1.0
Date Created	3rd March 2023
Next Review Date	4th March 2024

Change Control

Change Initiator	
Summary of Change	

DOCUMENT HISTORY

Revision History

Prepared/Updated By:	Version	Details of Content/Revision	Date

Distribution List

Title	Date

APPROVAL

Title	Name	Signature
Managing Director/CEO	Kayode Ayo	

BOARD APPROVAL PAGE

Title	Name	Signature

Information Security Policies

Internal Use **Version 1.0**

1 Introduction

It is the policy of Spoutpay Limited to ensure that pertinent documented information are properly identified, updated, approved and made available when needed.

This document defines the procedures on the control of documented information within Spoutpay Limited to ensure that appropriate versions of documented information are identified and made available when needed. It also aims to ensure that documented information of external origin is identified, and their distribution controlled.

1.1 Purpose

The purpose of the policies is to provide definitive statements which all Spout Pay's stakeholders are expected to comply with. This document is created to the acquaint all Spout Pay's stakeholders with information security risks and the expected ways to address these risks.

Also, this documents also help clarify all stakeholders' responsibilities and duties with respect to the protection of the Spout Pay's information resources. These policies also enable Spout Pay management and other stakeholders to make appropriate decisions about information security.

This Policies also coordinate the efforts of different departments within the Spout Pay and other stakeholders so that information resources, Spout Pay assets, applications and systems are properly and consistently protected, regardless of their location, form, or supporting technologies.

This policy applies to all stakeholders of Spout Pay and others who handle or managed its information including clients, contractors, consultants, and visitors of the company.

The policy relates to information managed or associated with Spout Pay, whether it is being stored or processed by the organization and which is held by employee's equipment or privately owned equipment's.

The policy covers all information management and processing activities whether they are undertaken on or off Spout Pay premises and however the information is being accessed.

2 Information Security Policies

2.1 Cloud Computing Policy

1. Data belonging to Spout Pay must only be stored within the Spout Pay's approved cloud computing environment with the prior permission of the Technical Project Manager.
2. Where available, two factor authentication must be used to access all cloud services.
3. All Spout Pay data must be removed from cloud services in the event of a contract coming to an end for whatever reason.
4. All proposed changes to cloud security operations must be documented in detail.
5. Spout Pay must create and manage user accounts on the Amazon Cloud Service and G-Suite in line with SPL -ISMS-POL-Access Control Policy-V01.

2.2 Mobile Device Policy

Spout Pay seeks to protect its mobile devices and the data stored on them, from unauthorized access, use, disclosure, alteration, modification, deletion, destruction and/or removal.

The following policy has been documented by the Spout Pay:

1. Spout Pay's business should be conducted using the organization's asset.
2. Devices carrying important, sensitive or critical business information must not be left unattended and, where possible, must be physically locked away.
3. It is the responsibility of users of mobile devices to ensure that unauthorized people (including friends and family members) are not allowed access to the Spout Pay's information assets processed or stored on them
4. Spout Pay reserve the right (where legally permissible) to enforce security controls such as access control, malware protection software and encryption to minimize the risk to the company and customer information assets

In a situation where a user's mobile device got stolen, the user account IP address will be disabled on the VPN.

2.3 Bring Your Own Device (BYOD) Policy

1. To ensure the security of Spout Pay information, authorized employees must have anti-virus software installed on their personal mobile devices.

2. Management reserves the right to review or retain Spout Pay's-related data on personal devices or release the data to government agencies or third parties during an investigation or litigation.
3. Upon resignation or termination of employment, or at any time on request, the employee may be asked to produce the personal device for inspection.
4. If the device is lost or stolen, the owner must inform the Engineering Department as soon as possible, giving details of the circumstances of the loss and the sensitivity of the business information stored on it.
5. All Spout Pay's data on personal devices must be removed by the technical team upon the termination of employment.

2.4 Remote Working Policy

A teleworking arrangement is a voluntary agreement between Spout Pay and the employee. It usually involves the employee working from home in a separate area of their living accommodation, whether this is a house, apartment, or other types of domestic residence.

The following policy are in place:

1. While working remotely, employees must take steps to preserve the security and confidentiality of Spout Pay's information.
2. Employees must keep confidential documents and materials in secure locations.
3. Employees must maintain password protection to the same extent as required at the workplace, and keep confidential documents and records securely stored.
4. If working on personal devices, employees must have valid up-to-date anti-virus software and appropriate computer and internet security installed and activated.
5. Any suspected hacks or breaches of security must be reported to the Engineering Department immediately.

2.5 Information Security in Project Management Requirement

1. Project and initiatives shall take into consideration the integrated management system objective and information security policies of Spout Pay regardless of the type of project.
2. To avoid potential breaches, all risk, threat and vulnerabilities identified with respect to a project must be treated in line with existing Spout Pay information security policies.
3. Information security implications shall be addressed and reviewed regularly through-out the project lifecycle.

4. All external and internal stakeholders participating in projects will sign a Non-Disclosure Agreement (NDA) to maintain the confidentiality and integrity of client information asset
5. Data Protection Impact Assessment (DPIA) shall be done for High-risk project. This is to be done to assist in identifying and minimizing the data protection risks of a project. DPIA must be done for processing that is likely to result in a high risk to individuals.

2.6 Physical Media Transfer Policy

The primary area of concern is the secure management of media to protect sensitive or personal information from intentional or accidental exposure or misuse. The following shall be implemented:

1. All staff handling Spout Pay-sensitive data must get approval for all physical media data transfers from their Line Manager.
2. When dealing with third parties, consider whether any data-sharing agreements or contracts are in place that covers the transfer of that data.
3. For all transfers of information containing personal or sensitive data, it is essential that you appropriately establish the identity and authorization of the recipient.
4. Legal advice should be sought to ensure compliance before media containing encrypted information or cryptographic controls are moved across jurisdictional borders.
5. The Technical Project Manager must be informed if physical media is lost or damaged during the transfer process.

2.7 Access Control Policy

Spout Pay views corporate information as the property of the organization and requires management and staff to control the access to information to protect it from accidental or unauthorized disclosure, modification or destruction. This policy covers all information that is held, processed, transmitted, or printed by any information processing facility.

The following guiding principles apply:

1. Access to corporate information shall only be given to users with a genuine need to conduct Spout Pay's business, implementing the Need-to-Know' and 'Need-to-Use' principles.
2. Information classification of information assets is a prerequisite - access rights and control shall be assigned and implemented in line with business risk

3. Individual accountability must be achieved, segregation of duties promoted and additional controls over users with special access privileges must be applied through access control mechanisms.
4. Spout Pay shall review and monitor any access logs when necessary.
5. Access rights or privilege given but no longer required shall be revoked and amended appropriately

2.8 Password Policy

The following rules are based on guidance from the UK NCSC (National Cyber Security Centre) and the USA National Institute of Standards and Technology (NIST). Where possible, passwords will have the following characteristics:

1. Require a minimum length of at least eight characters
2. Password complexity requirements will be used (e.g., specifying that a password must contain alphabets, special characters and numbers)
3. After Three unsuccessful login attempts are made, the user account will be locked out for about 30mins or will need to be re-enabled by an administrator
4. Password expiry of about 60 days
5. System default accounts/passwords will be disabled/changed immediately as part of the initial setup and configuration

2.9 Cryptographic Policy

In general, the policy of the Spout Pay is to use the following techniques for the relevant business process or situation:

1. For Spout Pay data stored on cloud, the technique to be employed is AES-256 encryption at rest
2. For Website Hosting, the technique to be used are either TLS 1.2 or AES 256
3. For E-Commerce transactions over the Internet, technique to be used is a Symmetric encryption using TLS (Asymmetric techniques used to share session key)
4. For Email Security, the technique to be adopted is the Symmetric/asymmetric encryption using S/MIME
5. For remote access, the encryption technique to be used on the Virtual Private Network (VPN) should be using TLS 1.2 or higher

2.10 Physical Access and Environmental Policy

1. Everyone visiting the Spout Pay's facility must wear an identification badge/tag on their outer garments to make the information on the badge visible.
2. The key to the office space must be held centrally by an assigned owner.

3. Laptop users are responsible for the security and use of their laptops and must exercise due care to prevent the theft or compromise of these devices.
4. Walls surrounding computer facilities must be non-combustible and resistant to fire.
5. Sufficient environmental control measures have been implemented to protect Spout Pay assets from preventable service disruptions or harm.

2.11 Clear Screen and Clear Desk Policy

All Spout Pay staff and others with access to classified information must take care to ensure that unauthorized people do not have access to it by being able to view it either on paper, on removable media, or a user's computer screen.

The following policy has been developed:

1. All sensitive or critical business information must be locked away when not in use.
2. You must not use or store anything under or on top of the desks.
3. All User must lock their screen (using Windows + L shortcut) whenever leaving their PC unattended.
4. Systems must be set to automatically lock the screen whenever idle for 5 minutes.
5. Computers must be logged off or protected with screen and keyboard logging mechanisms controlled by password, token or similar security solutions.

2.12 Software Policy

1. All installed software programs will be registered in the name of Spout Pay, not the individual.
2. All computer software to be used within Spout Pay must be purchased through Spout Pay's Engineering and Finance Department.
3. Licensed software will be installed by the Engineering department or appropriate technical team or supplier upon request and once any required licenses have been purchased.
4. Whether software is purchased or developed in house it is vital that it incorporates security throughout the software-development life cycle.
5. Strong cryptographic technology is incorporated within the software for data in transit and at rest where appropriate

2.13 Anti-Malware Policy

Anti-malware protection is vital to protect Spout Pay from viruses. Spout Pay must. identify, adopt and implement an antivirus solution to protect the Organisation against virus attacks.

The following policy address Anti-malware Policy:

1. All Spout Pay production and non-production systems and servers must have anti-virus protection software installed. The anti-virus software must be configured to automatically scan all files for malicious code.
2. Users must not, under any circumstance, disable or tamper with the antivirus software/configurations.
3. Users cannot uninstall nor can they stop any anti-virus-related services. Users can setup a custom scan of their own machine
4. URL filtering shall be implemented on the firewall, which is configured to filter the following categories: Full Nudity, Gross Depictions, Partial Nudity, Racism/Ethnic Impropriety, and sexual Acts.
5. All employees must notify the Engineering Department of any virus found by the anti-virus software

2.14 Back Up and Restore Policy

Spout Pay has established this Backup and Restore Policy to ensure the effectiveness of backup and restore operations through an established plan.

The following policy address Backup and Restore Policy:

1. Data Owners shall be responsible for ensuring that information under their control is backed-up appropriately to ensure business continuity in the case of any disaster or theft.
2. Engineering Department shall ensure that backup data are protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.
3. Systems backup must also be carried out immediately after any upgrade, or changes were done to a system or an application.
4. In the event of system failure, escalation procedures must be in place and made aware to system administrators.
5. A quarterly Backup Report must be maintained.

2.15 Capacity Management Policy

The provision of effective IT services depends on the availability of sufficient resources of several types, including technical, information, and financial. A process must be in place to understand the future requirements for capacity.

The following policy address Capacity Management Process:

1. Capacity and performance requirements will be agreed upon with the customer and interested parties
2. Capacity will be planned to meet the identified requirements and provide the level of service agreed in the SLA
3. Resource usage and performance will be monitored regularly on a frequency appropriate to act as a firm foundation for capacity planning
4. A documented, up to date capacity plan will be maintained for all services and resources within the scope
5. Changes to the capacity required should follow the change management process, and be communicated with enough notice to allow the cost-effective provision of additional capacity in line with the organizational budgeting cycle

2.16 Network Policy

This Network Security Policy sets out the Spout Pay overall approach to the maintenance of the integrity, confidentiality and availability of its information technology infrastructure and sets out the responsibilities for ensuring compliance with this guidance.

The following policy address Capacity Management Process:

1. A "Defense in Depth" approach will be adopted to network security whereby multiple layers of controls are used to ensure that the failure of a single component does not compromise the network.
2. The principle should be adopted that a network should consist of a set of smaller networks segregated from each other based on either trust levels or organizational boundaries (or both).
3. At all perimeters between the internal network and an external network (such as the Internet) effective measures should be put in place to ensure that only authorized network traffic is permitted.
4. Where information is to be transferred over a public network such as the Internet, strong encryption via SSL/TLS 1.2(or higher) must be used to ensure the confidentiality of the data transmitted.
5. Network Address Translation (NAT) will always be used when communicating to untrusted networks to ensure that private IP addresses are not disclosed.

2.17 Information Transfer Policy

Spout Pay recognizes its responsibility to process its information correctly and in line with all legal, regulatory, and internal policy requirements. The following policy

has been put in place to ensure appropriate control of information transfer in Spout Pay:

1. All information transferred must be done using an approved secure transfer process
2. All Information must be transferred using the Spout Pay's G-mail addresses and Slack.
3. All staff must not assume that the information requester is authorized or legally entitled to have it. If in doubt, staff should confirm with their line manager/Team Lead.
4. You must not release Spout Pay's confidential and secret information to unauthorized persons. This can open Spout Pay to legal sanction or litigation.
5. Removable devices must be scanned for viruses and malware in cases where they are used for information transfer

2.18 Electronic Messaging Policy

Spout Pay has established an Electronic Messaging Policy to help facilitate and conduct all electronic messaging systems of the Organization.

The following policy address Electronic Messaging in Spout Pay:

1. The Organisation has approved the use of Gmail as its official electronic messaging and must always be used when communicating with others on official business. You must not use a personal e-mail account for this purpose.
2. All messages sent from Spout Pay's provided e-mail address remain the property of Spout Pay and are part of the corporate record.
3. Issuing Spout Pay's email address to any subscriber list or posting on the Internet without prior authorization is forbidden.
4. Users are prohibited from using the Spout Pay's electronic mail systems for charitable endeavors, private business activities, religious, political or amusement/entertainment purposes.
5. All emails with file attachments must always be scanned for possible viruses or other malicious code before opening them.
6. Spout Pay's sensitive information must not be forwarded to any party outside Spout Pay without the prior approval of the relevant Departmental Head.
7. Users must ensure the information they are forwarding by e-mail is correctly addressed and only being sent to intended recipients.
8. Encryption must be put in place for secure transmission of confidential and secret emails to third parties, partners and customers.

9. Users must not access another user's electronic messaging account unless they have obtained permission from the owner of the account or their line manager.
10. If you believe you have a virus or you have been sent an e-mail that may contain one, you must report this to the Engineering Department immediately.

2.19 Third Party Information Security Policy

Spout Pay relationships with third parties are based on a clear understanding of its expectations and requirements in the area information security. These requirements have been documented and agreed in a way that leaves no doubt about the importance we place on the maintenance of effective controls to reduce risk.

The following policy address Third party information security in Spout Pay:

1. A due diligence exercise must be completed by an authorized business area/department for all third parties who will access or could potentially access Spout Pay information.
2. Contracts with third parties accessing Spout Pay information must clearly state their obligations in terms of protecting information assets.
3. Formal third-party risk assessments for all high risk third parties must be updated at least every 12 months if the contract period is longer than one year.
4. Changes to third party contracts or service level agreements must be managed through a formal change management process.
5. The use of third-party cloud computing services is subject to the same controls as other third-party services.

2.20 Data Retention and Protection Policy

Spout Pay collects and stores records of many types and in a variety of different formats in its everyday business operations. The importance and sensitivity of these records also varies, and it is subject to the organization's security classification scheme (see *Information Classification Procedure*).

The following policy address Data Retention and Protection Policy in Spout Pay:

1. Records should be held in compliance with all applicable legal, regulatory, and contractual requirements
2. Records should not be held for any longer than required
3. The protection of records in terms of their confidentiality, integrity and availability should be in accordance with their security classification
4. Records should always remain retrievable in line with business requirements.

5. Sensitive records should not be recoverable when deleted electronically and physically in line with standard requirement.

2.21 IP and Copyright Compliance Policy

Intellectual property rights are very important to protect Spout Pay's assets that can be vital to the products or services, or the success and profitability of the business.

The following policy address IP and Copyright Compliance in Spout Pay:

1. Any products developed by Spout Pay's Staff during their contracted work and/or using Spout Pay assets are by default considered IP of Spout Pay unless different arrangements between the author(s) and the organization were made before performing the work
2. Before using any software, Spout Pay must obtain the necessary licenses or acquire IP rights based on sizing and identifying its business and operational requirements.
3. The software owner and Spout Pay must ensure that all usage activities regarding the IP comply with their licenses and copyright terms or other terms on using and/or disposing of such IP.
4. In case of any doubts about the legitimate use of any Open-source software used within Spout Pay, it is the responsibility of the technical manager to clarify all the doubts and get possible support if necessary.
5. If employees have doubts about compliance with the right to use IP, they must confirm with the Engineering Department and, if necessary, the legal Department.

3 Policy Compliance

3.1 Compliance Measurement

The Engineering Team and Legal and Compliance Department will verify compliance to this policy through various methods, including but not limited to, periodic walk-through, business tool reports, internal and external audits, and inspection, and will provide feedback to the policy owner and appropriate business unit manager.

3.2 Exceptions

Any exception to the policy must be approved by Top Management before such exception will be granted.

3.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.